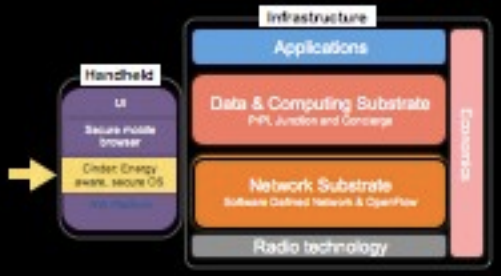
Rethinking the Handset Operating System

Arjun Roy, Stephen Rumble, Ryan Stutsman,
Philip Levis, and David Mazières

Cinder

- A new OS designed for mobile phones
- Goal: can download and run any code without worry
  - Track data, not code
  - Manage energy as a resource
- Start with a clean design, seek backwards compatibility later

POMI Research Agenda



UNIX, a Life

The Progression

1969 2009

Computing has Changed

- Commodity devices
- Rich, user-centric applications
- Battery-powered
- Untrustworthy programs

Research Synergy

- Cinder: an OS for mobile phones
- David Mazières: secure systems
- Philip Levis: energy-efficient systems
- These two goals can conflict
  - Cinder has explored this tension
  - More details later

Cinder Security

(a very brief overview)

Cinder Security

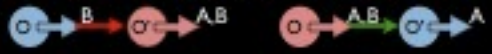
- Builds on HiStar operating system
- Every object has a label
  - Label has secrecy and integrity categories
- Kernel controls how information flows
  - "Flows-to" invariant based on labels

Information Flow

- Secrecy (read permission)
- Integrity (write permission)

- O with secrecy(A) cannot flow to O' without secrecy(A)

- O without integrity(A) cannot flow to O' with integrity(A)



Explicit Information Flow

- Labels make all information flow explicit
  - No covert channels
- Democratizes security control -- no "root" or "Administrator"
  - Simplifies delegation

Energy

A Personal Story

Some Examples

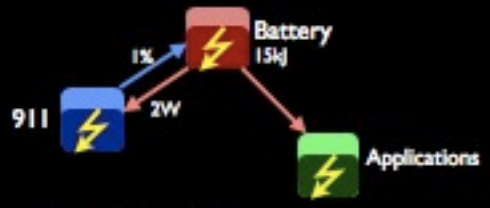
- Save energy for a 911 call
- Browser plugins do not starve browser
- Background email won't kill battery

Abstractions

- Reserves (vertices)
  - Contain energy
  - All threads run drawing from one or more
  - Battery is root reserve

- Taps (edges)
  - Draw power
  - Constant (1mW) or proportional (10%)

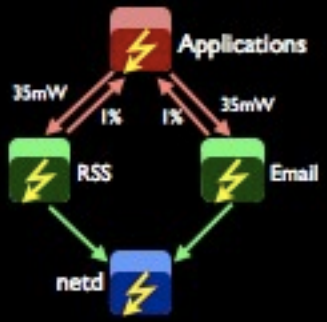
911 Call



200W = 5 minutes talk time

Browser Plugins

Email Check



Issue: Hoarding

- Application can hoard, starve system

Issue: Hoarding

- Application can hoard, starve system

Tension and Synergy

- Explored how to prevent hoarding
  - Require duplicating back edges on subdivision
  - Use "bogojoules," charge up hierarchy
- Tension between energy control and security (information flow)
  - Approaches above require read/write access to entire path in graph
- Cinder approach: global "half life"

Current Status

- Cinder boots on an Android G1 phone
- Device support
  - Frame buffer, serial port
  - Phone calls, SMS
- Capacitors operational
- Submission to OSDI

Moving Forward

- Phones are closed devices
  - Conflict between research and protection
  - E.g., Qualcomm likes Cinder, can't help us
  - Pain is above student threshold (> 1 year)
  - Exploring other collaborations (Google)
- Researchers need an open phone platform
  - Proposal with Michigan, Brown (resubmitting)

Questions